AMENDMENTS TO THE SPECIFICATION

In page 21, line 9, please amend the specification as reflected in the following marked-up version of the paragraph:

The data structure 500 of the request may include an eXtensible Markup Language (XML) element or any other data structure that identifies the authentication methods and the computer systems and/or users to which those authentication methods will be applied. Take the following XML element as an example.

```
<?xml version="1.0"?>
<a:rvpacl xmlns:a="~~http://schemas.microsoft.com/rvp/acl/~~Schema URL">
    <a:acl>
        <a:inheritance>none</a:inheritance>
        <a:ace>
            <a:principal>
                <a:rvp-principal>
                ~~http://im.example.com/instmsg/aliases/220b/~~"Aliases URL"
                </a:rvp-principal>
                <a:credentials>
                    <a:digest/>
                    <a:ntlm/>
                </a:credentials>
            </a:principal>
        </a:ace>
    </a:acl>
</a:rvpacl>
```

In page 22, line 8, please amend the specification as reflected in the following marked-up version of the paragraph:

In this XML element, the portion between <a:acc> and </a:ace> defines an Access Control Element (ACE) that defines access permissions. This portion would correspond to the access control element field 510a shown in Figure 5. The portion of the access control element that occurs between <a:rvp-principal> and </a:rvp-principal> defines the entity to whom the access permission is to apply (corresponds to the client identifier field 512 of Figure 5). In the above example request, the Aliases Uniform Resource Locator (URL) corresponding to the entity ~~is "http://im.example.com/instmsg/aliases/220b/" which~~ represents client computer system 220b. The portion of the access control element that occurs between <a:credentials> and </a:credentials> describes authentication mechanisms that may be used to authenticate the client computer system 220b when requesting access to services (corresponds to the authentication field 514 of Figure 5). This portion describes the two authentication methods that may be used when authenticating the client computer system 220b. Specifically, "<a:digest/>" means that the "digest" authentication method is acceptable while "<a:ntlm/>" means that the "ntlm" method is also acceptable.